CLAIMS

What is claimed is:

1. A system for generating, installing to a plurality of linked remote computers, and monitoring a secure network of nodes, said system comprising:

   A. at least one software application;

   B. an installation server, configured to facilitate installation of said at least one software application;

   C. a generator, configured to generate a plurality of software components from a network definition, including a plurality of agent modules, wherein each agent module is executable on a corresponding remote computer to initiate communication with said installation server and subsequent installation of a corresponding software application on said remote computer to form a node, wherein each of said nodes is capable of automatically establishing communication with others of said nodes according to said network definition; and

   D. a monitor node configured to monitor security of said network.

2. A system according to claim 1, wherein the remote computers are linked substantially by the Internet.

3. A system according to claim 1, wherein the remote computers are linked substantially by an intranet.

1   4.   A system according to claim 1, wherein said network definition includes a plurality of

2   node definitions, each node definition including:

3   C.   (i)   an identification of one of said plurality of remote computers;

4   (ii)   an identification of at least one software application to be installed on said

5   remote computer to form a node; and

6   (iii)   an identification of each other node to which said node is to be linked.

1   5.   A system according to claim 4, wherein said identification of each of said plurality

2   remote computers includes:

3   C.   (i)   (a)   an IP address; and

4   (b)   a node name.

6.   A system according to claim 1, wherein said plurality of software components further

includes:

C.   (i)   a plurality of node configuration files, wherein a different one of said node

configuration files corresponds to a different node and includes

information for facilitating selective communication with others of said

nodes according to said network definition; and

(ii)   at least one network information file, having information corresponding to

substantially all links between nodes and accessible by said monitor node

to facilitate the selective linking of said nodes.

1   7.   A system according to claim 1, wherein said installation server is configured to facilitate

2   said installation of said corresponding software application as a function of a verification

3   that said agent module is executing on said corresponding remote computer, according to

4   said network definition.

1   8.   A system according to claim 1, wherein said installation server is configured to facilitate

2   said installation of said corresponding software application as a function of a verification

3   that said agent module has not been previously installed.

9.   A system according to claim 1, further including a second monitor node configured to

      determine the presence of an interposed, unintended node.

10.   A system according to claim 1, wherein said monitor node is further configured to

      selectively terminate operation and connection of one or more tainted nodes in response

      to a detected security violation.

1   11.   A system according to claim 10, wherein said installation server is further configured to

2   initiate a regeneration of a set of said software components, reinstallation of said at least

3   one software application, and selective relinking to other nodes for each of said

4   selectively terminated one or more tainted nodes and according to said network

5   definition.

1   12.   A system according to claim 1, wherein said monitor node and each of said nodes

2   communicate using secure data transfer.

1   13.   A system according to claim 12, wherein said secure data transfer is accomplished using

2   data encryption, and wherein data transferred in each direction between two linked nodes

3   is encrypted differently.

1   14.   A system according to claim 13, wherein each of two linked nodes uses a unique pair of

2   encryption keys to accomplish said data encryption, and each pair of encryption keys

3   includes a substantially hidden private key and a public key.

1   15.   A system according to claim 14, wherein said monitor node is further configured to

2   selectively initiate a coordinated strobing of each pair encryption keys between two linked

3   nodes.

1   16.   A system according to claim 1, further including:

2   E.   an account server, configured to generate billing information as a function of the

3   selective linking of said node to said other nodes.

1   17.   A system according to claim 1, wherein said installation server is configured to

2   communicate with each of said plurality of remote computers using data encryption.

1   18.   A system according to claim 17, wherein said installation uses a randomly generated

2   private key and public key pair for data encryption, wherein data to be transferred to said

3   installation server is encrypted using said public key and is decrypted by said installation

4   server using said private key.

1   19.   A system according to claim 18, further including:

E.   a second monitor node, configured to compare the installation server public key

with the encryption key used by one of said plurality of remote computers to

encrypt data sent to said installation server, a negative comparison being

indicative of a security violation.

20.   A system for generating, installing to a plurality of linked remote computers, and

monitoring a secure network of nodes, said system comprising:

A.   at least one software application;

B.   an installation server, configured to facilitate installation of said at least one

5   software application;

6   C.   a generator, configured to generate a plurality of software components from a

7   network definition, including a plurality of agent modules, wherein each agent

8   module is executable on a corresponding remote computer to initiate

9   communication with said installation server and subsequent installation of a

10   corresponding software application on said remote computer to form a node,

11   wherein each of said nodes is capable of automatically establishing

12   communications with others of said nodes according to said network definition;

13   and

14   D.   a monitor node configured to monitor security of said network, wherein said

15   monitor node and each of said nodes communicate using secure data transfer.

21.   A system according to claim 20, wherein said secure data transfer is data encryption and

       each of two linked nodes uses a unique set of encryption keys to accomplish said data

3   encryption.

22.   A system according to claim 21, wherein said encryption keys are substantially randomly

       generated.

23.   A system according to claim 21, wherein each set of said encryption keys includes a

       hidden private key and a public key, and said public key is used by a first node in a link to

3   encrypt data transmitted to a second node in the link, and said private key is used to

4   decrypt said data by said second node.

1   24.   A system according to claim 21 wherein said monitor node is further configured to

2   selectively initiate a coordinated strobing of each set of encryption keys between two

3   linked nodes.

1   25.   A system according to claim 21, wherein said monitor node is further configured to

2   effectuate persistence of said encryption keys, and wherein when a first set of encryption

3   keys used by two linked nodes is strobed, a second set of encryption keys is randomly

4   generated, and said first and said second sets are stored in a memory, such that when one

5   or both of said two linked nodes loses its connection with the other of said two linked

6   nodes , said two linked nodes attempt to reestablish said connection alternatively using

7   said first and said second set of encryption keys.

1   26.   A system according to claim 21, wherein said installation server is configured to

2   communicate with each of said plurality of remote computers using data encryption.

1   27.   A system according to claim 26, wherein said installation uses a randomly generated

2   private key and public key pair for data encryption, wherein data to be transferred to said

3   installation server is encrypted using said public key and is decrypted by said installation

4   server using said private key.

1   28.   A system according to claim 27, further including:

2   E.   a second monitor node, configured to compare the installation server public key

3   with the encryption key used by one of said plurality of remote computers to

4   encrypt data sent to said installation server, a negative comparison being

5   indicative of a security violation.

1   29.   A system for generating, installing to a plurality of linked remote computers, and

2   monitoring an auditible secure network of nodes, said system comprising an secure

3   network:

4   A.   at least one software application;

5   B.   an installation server, configured to facilitate installation of said at least one

6   software application;

7
8   C.   a generator, configured to generate a plurality of software components from a

9   network definition, including a plurality of agent modules, wherein each agent

10   module is executable on a predetermined corresponding remote computer to

11   initiate communication with said installation server and subsequent installation of

12   a predetermined corresponding software application on said remote computer to

13   form a node, wherein each of said nodes is capable of automatically establishing

14   communication with others of said nodes according to said network definition,

15   and wherein said subsequent installation is contingent upon a first verification that

16   said agent module is installed on its corresponding remote computer and wherein

17   said installation is further contingent upon a second verification that said software

18   application is installed on its predetermined corresponding remote computer; and

            D.   a monitor node configured to monitor security of said network.

1   30.   A system according to claim 29, wherein said installation server is configured to

2   terminate said installation of said at least one software application on said corresponding

3   remote computer if said agent module has been previously installed.

1   31.   A system according to claim 29, wherein said installation server is configured to

2   terminate said installation of said at least one software application on said corresponding

3   remote computer if said agent module is not installed on said corresponding computer.

1   32.   A system according to claim 29 wherein said installation server is configured to perform

2   said subsequent installation in response to receipt of a password entered at said remote

3   computer, as said first verification.

.33.   A system according to claim 29, wherein said installation server is configured to

        complete said installation in response to receipt of a password entered at said remote

        computer, as said second verification.

.34.   A system according to claim 29, further including:

        E.   a software component analyzer, configured to analyze said software components

                and determine the presence of trap doors.

1   35.   A system according to claim 29, wherein said installation server is configured to

2   communicate with each of said plurality of remote computers using data encryption.

1   36.   A system according to claim 35, wherein said installation uses a randomly generated

2   private key and public key pair for data encryption, wherein data to be transferred to said

3 installation server is encrypted using said public key and is decrypted by said installation

4 server using said private key.

1 37. A system according to claim 36, further including:

2 E. a second monitor node, configured to compare the installation server public key

3 with the encryption key used by one of said plurality of remote computers to

4 encrypt data sent to said installation server, a negative comparison being

5 indicative of a security violation.

38. A method for generating, installing to a plurality of remote computers, and monitoring a

secure network having a plurality of nodes, a generator, an installation server, and a

monitor node, the method comprising the steps:

4 A. creating a network definition, including information that describes each remote

5 computer, at least one software application to be installed on each remote

computer, and each link between nodes;

7 B. generating with said generator a plurality of software components, as a function of

8 said network definition, including a plurality of agent modules, wherein each

9 agent module is executable on a preselected one of said remote computers and

10 includes functionality to communicate with said installation server;

11 C. executing an agent module on its corresponding remote computer, wherein said

12 agent module automatically establishes communication with said installation

13 server;

14   D.   downloading, using said installation server, to said remote computer a

15   corresponding at least one software application;

16   E.   executing said at least one software application on said remote computer to form a

17   node and automatically establishing a connection with said monitor node;

18   F.   selectively linking said node to others of said plurality of nodes according to said

19   network definition; and

20   G.   repeating steps C through F for each agent module and corresponding remote

          computer.

39. The method of claim 38, wherein step A includes identifying each remote computer by an

     IP address and a node name.

40. The method of claim 38 wherein step B further includes generating:

          (i)   a plurality of node configuration files, wherein each node configuration

                file corresponds to one of said nodes; and

          (ii) a set of network information files, including information corresponding to

                a plurality of links required to form said network.

41. The method of claim 38 wherein step D further includes verifying that said agent module

     is executing on a corresponding remote computer, according to said network definition,

     as a prerequisite to downloading said at least one software application.

1   42.   The method of claim 41 wherein step B includes generating a unique local password for

2   each node and said verifying in step D includes:

3   (i)   entering said local password at said remote computer; and

4   (ii)   verifying said local password at said installation server.

1   43.   The method of claim 38 wherein step D further includes verifying that said agent module

2   has not been previously installed, as a prerequisite to downloading said at least one

3   software application.

44.   The method of claim 38 wherein step F further includes verifying that said software

application is executing on its corresponding remote computer according to said network

definition, as a prerequisite of selectively linking said node to others of said plurality of

nodes.

45.   The method of claim 44 wherein step B includes generating a unique audit password for

2   each node and said verification in step F includes:

3   (i)   entering said audit password at said remote computer; and

4   (ii)   verifying said audit password.

1   46.   The method of claim 38, further including a step:

2   H.   terminating operation and connection of one or more tainted nodes, under control

3   of said monitor node, in response to detection of a security violation related to

4   said tainted node.

1   47.   The method of claim 46, further including a step:

2   I.   repeating steps B-G for each of said one or more tainted nodes.

1   48.   The method of claim 38, wherein step B further includes generating for each node in a

2   pair of linked nodes, a set of encryption keys, including a private key and a public key, to

             facilitate secure communication between said linked nodes.

1   49.   The method of claim 48, further including step:

2   H.   (i)   selecting said pair of linked nodes; and

3   (ii)   strobing each set of encryption keys for said linked nodes.

1   50.   The method of claim 49, wherein said two linked nodes are a first node and a second

2   node and said strobing includes the steps:

3   (a)   ceasing data transfer between said first and second nodes;

4   (b)   randomly generating a new first private key for said first node;

5   (c)   deriving a new first public key from said new first private key and

6   storing said new first private and public keys;

7   (d)   encrypting said new first public key with a current second public

8   key of said second node and transmitting said new first public key

9   to said second node;

10   (e)   decrypting with a current second private key said new first public

11   key and storing said new first public key at said second node and

12   randomly generating a new second private key;

13   (f)   deriving a new second public key from said new second private

14   key and storing said new second private and public keys;

15   (h)   encrypting said new second public key with a current first public

16   key of said first node and transmitting said new second public key

17   to said first node;

18   (i)   decrypting with a current first private key said new second public

19   key and storing said new second public key at said first node;

20   (j)   exchanging confirmations between said first and second nodes to

21   use said new first and second private and public keys; and

22   (k)   resuming data transfer between said two linked nodes.

51.   The method of claim 50, wherein each pair of linked nodes also uses at least one session

     key to encrypt data transferred between said linked nodes and said strobing further

3   includes:

4   randomly generating, exchanging and storing at least one new session key for said

5   linked nodes, between steps H(ii)(a) and H(ii)(k).

1   52.   The method of claim 50 wherein said strobing is strobing with persistence and said step

2   H(ii) further includes saving said current first and second public and private keys.

1   53.   The method of claim 38, wherein said network further includes an account server, said

2   method further comprising the step of:

3   H.   (i) communicating to said account server said linking of said node, in step F; and

4   (ii) generating billing information related to said linking of said node.

1   54.   The method of claim 38, wherein step B includes generating a unique set of encryption

2   keys for each node and said monitor node.

1   55.   The method of claim 54, wherein step E includes the steps of:

2   (i)   logging into said monitor node by said node using a unique encryption key from a

3   corresponding set of node encryption keys generated by said generator; and

4   (ii)   logging into said node using a unique monitor node encryption key from a

5   corresponding set of monitor node encryption keys generated by said generator.

1   56.   The method of claim 38, wherein said secure network further includes a second monitor

2   node and said installation server communicates with each of said plurality of remote

3   computers using a private and public encryption key pair, the method further including

4   the step of:

5   H.   (i)   comparing the public key of said installation server with a key used by one

6   of said plurality of remote computers to encrypt data sent to said

7   installation server; and

8   (ii)   issuing a security violation message, in the event of a negative

9   comparison.

1   57.   A method for generating, installing to a plurality of remote computers, and monitoring a

2   secure network having a plurality of nodes, a generator, an installation server, and a

3   monitor node, said network used for conducting financially related transactions between a

4   custody system of a bank and a trading system of a financial client, the method

5   comprising the steps of:

        A.   creating, by a bank sales department, a network definition embodying the network

   7   required by the financial client and to be generated, installed and monitored by the

   8   bank;

   9   B.   modeling and testing said network definition, by a bank development group;

10   C.   obtaining authorization from a bank network administration group and installing

11   said network definition on said generator, by said bank development group;

12   D.   obtaining by said bank sales group a sales password and authorization to install

13   network from said network administration group;

14   E.   auditing on said generator a generated network definition by comparing said

15   generated network definition to said network definition and inputting said sales

16   password as an indication of a favorable comparison, by said bank sales group;

17   F.   obtaining by a bank audit group, an audit password and authorization to install

18   network from said network administration group;

19   G.   auditing on said generator a generated network definition by comparing said

20 generated network definition to said network definition and inputting said audit

21 password as an indication of a favorable comparison, by said bank audit group;

22 H. generating with said generator a plurality of software components to be installed

23 on said plurality of remote computers to form said plurality of nodes of said

24 network, said components including:

25 (i) a plurality of agent modules, each agent module having the capability to

26   establish communications with said installation server;

27 (ii) a local sales password, for each agent module;

28 (iii) a local audit password for each agent module;

29 I. registering said agent modules with said installation server, wherein said

30 installation server has access to at least one or more bank custody software

31 applications to be stored on each of said plurality of remote computers to form

32 said nodes, according to said network definition;

33 J. communicating to each remote computer a corresponding one of said local sales

34 passwords to a sales department representative;

35 K. communicating to each remote computer a corresponding one of said local audit

36 passwords to an audit department representative;

37 L. executing each agent module on its corresponding remote computer, entering said

38 local sales password to verify that said agent module is installed on its

39 corresponding remote computer according to said network definition, and

40 downloading said corresponding at least one bank custody software application;

41 M. executing each of said at least one software applications on its corresponding

42   remote computer, establishing communication with said monitor node, entering

43   said local audit password to verify that said at least one software application is

44   installed on its corresponding remote computer according to said network

45   definition; and

46   N.   selectively linking said nodes into said network.

58.   A method for generating, installing to a plurality of remote computers, and monitoring a

secure network having a plurality of nodes, a generator, an installation server, and a

monitor node, wherein the secure network is used for the exchange of confidential data

between a first system of a first group and a second system of a second group, the method

comprising the steps:

A.   creating a network definition, including information that describes each remote

        computer, at least one first group software application to be installed on each

        remote computer, and each link between nodes;

B.   generating with said generator a plurality of software components, as a function of

        said network definition, including a plurality of agent modules, wherein each

        agent module is executable on a preselected one of said remote computers and

        includes functionality to communicate with said installation server;

C.   executing an agent module on its corresponding remote computer, wherein said

        agent module automatically establishes communication with said installation

        server;

D.   (i)   human auditing and verifying that said agent module is installed on its

17			corresponding remote computer according to said network definition by a
18			third group; and
19		(ii)	downloading, using said installation server, to said remote computer a
20			corresponding at least one first group software application;
21	E.	(i)	executing said at least one first group software application on said remote
22			computer to form a node and automatically establishing a connection with
23			said monitor node; and
24		(ii)	human auditing and verifying that said at least one first group software
25			application is installed on its corresponding remote computer according to
26			said network definition by a fourth group, independent from said third
27			group;
28	F.		communicating with others of said plurality of nodes according to said network
29			definition; and
30	G.		repeating steps C through F for each agent module and corresponding remote
31			computer.

33   59.   The method of claim 58 wherein said confidential data is financial data and said first

34   system of said first group is a custody system of a bank and said second system of said

35   second group is a trading system of a financial services group.